JD Edwards EnterpriseOne

Application Interface Services Server for Mobile Enterprise Applications Configuration Guide

Tools Release 9.1.x

E51517-07

July 2015

Describes the configuration of the Application Interface Services (AIS) Server which provides the communication interface between JD Edwards EnterpriseOne mobile enterprise applications and JD Edwards EnterpriseOne.

JD Edwards EnterpriseOne Application Interface Services Server for Mobile Enterprise Applications Configuration Guide, Tools Release 9.1.x

E51517-07

Contents

4 Troubleshooting Mobile Enterprise Applications

Preface

Welcome to the *JD Edwards EnterpriseOne Application Interface Services Server for Mobile Enterprise Applications Configuration Guide*.

> **Note:** This guide has been updated for JD Edwards EnterpriseOne Tools 9.1 Update 4.2, 9.1 Update 4.6, 9.1 Update 5, and 9.1 Update 5.5.

Audience

This document is intended for administrators who have experience with setting up and administering the EnterpriseOne system. In particular, you should have experience using Server Manager to deploy and manage server instances and EnterpriseOne administration applications to set up security and processing options.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

This guide also contains references to additional implementation instructions in the following guides:

- *JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implementation Guide*
- *JD Edwards EnterpriseOne Tools Server Manager Guide*
- *JD Edwards EnterpriseOne Tools Security Administration Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

This chapter contains the following topics:

- Section 1.1, "Overview"
- Section 1.2, "Configuration Checklist"
- Section 1.3, "Accessing Minimum Technical Requirements (Certifications)"

1.1 Overview

This guide describes the configuration of the Application Interface Services (AIS) Server which provides the communication interface between JD Edwards EnterpriseOne mobile enterprise applications and JD Edwards EnterpriseOne. It also contains information about additional setup tasks that must be performed in EnterpriseOne to determine the data that mobile users can access and work with in mobile enterprise applications.

This guide also contains references to additional mobile enterprise applications implementation instructions located in the *JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implementation Guide*.

1.2 Configuration Checklist

As you read through the contents of this guide and the *JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implementation Guide*, use the following list of tasks as a checklist for setting up mobile enterprise applications:

- Deploy the AIS Server through Server Manager.
- Configure the Allowed Hosts setting for the EnterpriseOne HTML Server.
- Verify JAVA argument for AIS Server (Oracle WebLogic Server Only).
- Define mobile enterprise application versions for mobile users.
- Specify processing options and display options for mobile enterprise applications.
- Set up security for mobile enterprise application versions.
- Set up security for base EnterpriseOne applications used by mobile enterprise applications.

1.3 Accessing Minimum Technical Requirements (Certifications)

The following list contains references to the minimum technical requirements for the AIS Server for mobile:

- Customers must conform to the supported platforms for the AIS Server, which can be found in the Certifications tab on My Oracle Support: `https://support.oracle.com`.

  For more information about JD Edwards EnterpriseOne Minimum Technical Requirements, see the following document on My Oracle Support:

  JD Edwards EnterpriseOne Minimum Technical Requirements Reference (Doc ID 745831.1)

  `https://support.oracle.com/epmos/faces/DocumentDisplay?id=745831.1`

- For a list of the EnterpriseOne mobile enterprise applications and the minimum EnterpriseOne Tools release required to run them, see the following document on My Oracle Support (login required):

  Information Center for JD Edwards EnterpriseOne Mobile Applications (Doc ID 1637232.2)

  `https://support.oracle.com/epmos/faces/DocumentDisplay?id=1637232.2`

2 Configuring the Application Interface Services Server

This chapter contains the following topics:

2.1 Overview of the AIS Server Configuration for EnterpriseOne Mobile Enterprise Applications

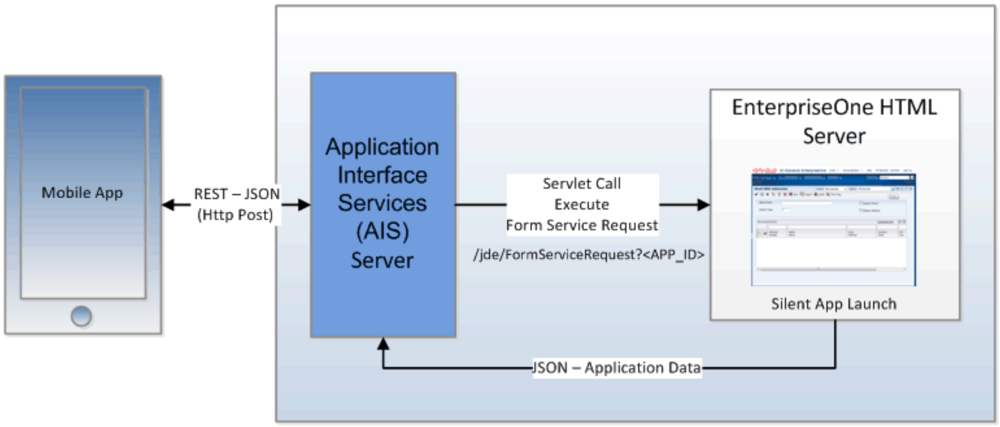
EnterpriseOne mobile enterprise applications require a light interface to manage EnterpriseOne data from mobile devices. The Application Interface Services (AIS) Server provides a JSON over REST interface to EnterpriseOne applications and forms through the EnterpriseOne HTML Server. The AIS Server exposes this interface to enable communication between mobile applications and EnterpriseOne.

The AIS Server includes support for JSON representation of form service requests so mobile applications can easily format requests. The AIS Server submits these mobile application requests to the EnterpriseOne HTML server.

The AIS Server maintains sessions for mobile applications. You can configure the session timeouts for the AIS Server through Server Manager.

The following illustration shows how the AIS Server functions as the interface between mobile applications and the EnterpriseOne HTML Server.

Figure 2–1 JD Edwards EnterpriseOne AIS Server for Mobile Architecture



2.2 Deploying and Managing the AIS Server through Server Manager

Deploy the AIS Server as a managed instance through Server Manager. You can deploy the AIS Server on Oracle WebLogic Server or IBM WebSphere Application Server.

When deploying the AIS Server, remember the server name and port number. These values make up the URL that you need to provide to mobile users, for example: `http://<ais_servername>:<portnumber>`. The first time mobile users launch a mobile enterprise application, they are prompted to enter this URL to access the application.

For instructions on how to deploy the AIS Server as a managed instance, see "Create an Application Interface Services (AIS) Server as a New Managed Instance" in the *JD Edwards EnterpriseOne Tools Server Manager Guide*.

2.2.1 Managing the AIS Server through Server Manager

Server Manager provides settings and features that enable you to configure and manage the AIS Server. These include:

- Configuration group settings to determine whether the Environment and Role fields and the Single Sign On option are displayed or hidden on the mobile application login screen. The configuration group settings also include settings for controlling session timeouts and other configuration options.

  See "Configuration Groups" in the *JD Edwards EnterpriseOne Tools Server Manager Guide* for more information about configuration groups for all EnterpriseOne server types.

- Starting with Tools Release 9.1 Update 5, runtime metrics that show various user and server-related information, which enable you to view a list of users connected to the AIS Server and monitor user activity.

  See "Application Interface Services Server Runtime Metrics" in the *JD Edwards EnterpriseOne Tools Server Manager Guide* for more information.

- Starting with Tools Release 9.1 Update 5, configuration group settings for the AIS Server. These settings include display options, AIS Server and HTML Server communication options, security options, and logging options.

  See "EnterpriseOne Application Interface Services" in the *JD Edwards EnterpriseOne Tools Server Manager Guide* for more information.

2.3 Additional Required Server Configurations

After deploying the AIS Server through Server Manager, perform the following tasks in this section to complete the configuration between the AIS Server and EnterpriseOne HTML Server:

- Configuring the Allowed Hosts Setting for the EnterpriseOne HTML Server
- Verifying the JAVA Argument for AIS Server (Oracle WebLogic Server Only)
- Configuring SSL for the AIS Server
- Configuring Oracle WebLogic Server Domain for HTTP Basic Authentication (Release 9.1 Update 5.5)

2.3.1 Configuring the Allowed Hosts Setting for the EnterpriseOne HTML Server

In Server Manager, configure the Allowed Hosts setting for the EnterpriseOne HTML Server to specify the AIS Server host from which the EnterpriseOne HTML Server will receive requests.

1. In Server Manager, access the EnterpriseOne HTML Server managed instance.
2. Expand the Form Service area, and in the Allowed Hosts field, enter the IP Address of the AIS Server.
3. Restart the server for the changes to take effect.

> **Note:** If the mobile enterprise application fails to connect to the server, verify that the IP Address of the AIS Server has been entered correctly in the Allowed Hosts field. If the IP Address is correct and the connection still fails, then enter an * (asterisk) in the Allowed Hosts setting, which enables the EnterpriseOne HTML Server to accept requests from any host.

2.3.2 Verifying the JAVA Argument for AIS Server (Oracle WebLogic Server Only)

If the AIS Server is deployed on Oracle WebLogic Server, you must make sure that the server configuration includes a JAVA argument for starting the server. To do so:

1. In the WebLogic Admin Console, locate the AIS Server instance.
2. Click the **Server Start** tab.
3. Verify that the following argument is in the Arguments field:

   ```
   -DuseSunHttpHandler=true
   ```

2.3.3 Configuring SSL for the AIS Server

The availability of the AIS Server port number can enable mobile client access to the AIS Server without the use of a VPN. To protect information sent between the mobile client and the AIS Server, you should use SSL when configuring the AIS Server. If you enable the AIS Server for SSL (HTTPS), you must use a valid certificate. The encryption algorithm for the certificate must be one of these three types:

- Signature.MD2withRSA
- Signature.MD5withRSA
- Signature.SHA1withRSA

2.3.4 Configuring Oracle WebLogic Server Domain for HTTP Basic Authentication (Release 9.1 Update 5.5)

Starting with EnterpriseOne Tools Release 9.1.5.5, REST services on the JD Edwards EnterpriseOne AIS Server can use HTTP Basic Authentication for access. Support for HTTP Basic Authentication is enabled out of the box and is required to run the EnterpriseOne Orchestrator Client, create custom Java calls from orchestrations, and use the AIS client Java API (versions 1.2.1.x and higher).

If your AIS Server is deployed on Oracle WebLogic Server, the WebLogic Server may require an additional configuration depending on the WebLogic Server configuration.

If you are maintaining a user registry in Oracle WebLogic Server that matches the user registry in EnterpriseOne, with identical sets of user names and passwords in each system, you do NOT need to modify your configuration.

If you are NOT maintaining identical sets of users in Oracle WebLogic Server and EnterpriseOne, then you need to perform the following steps to modify your Oracle WebLogic Server configuration. This ensures that Oracle WebLogic Server will not intercept HTTP Basic Authentication credentials passed from the REST service.

1. In the WebLogic Server domain for your AIS Server, in the Config directory, find the config.xml file.
2. Add this configuration as the last line within the `<security-configuration>` element, just before the `</security-configuration>` tag:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-
   credentials>
   ```

3. Restart the AIS Server for the changes to take effect.

The following is an example of this configuration in the `<security-configuration>` element:

```
<node-manager-password-encrypted>{AES}tzAokzTHACTNNmkuutLPQEpP8bfk7Ble24vmoycooic=
</node-manager-password-encrypted>

<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
  </security-configuration>
  <server>
```

2.4 Remapping Fields for Customized EnterpriseOne Forms (Release 9.1 Update 4.6)

This section contains the following topics:

- Overview
- Using the JDE JSON Mapping Tool to Map Mismatched Fields
- Modifying and Deploying AIS Field Mappings

2.4.1 Overview

If an EnterpriseOne mobile enterprise application invokes an EnterpriseOne form that has been customized, the mobile enterprise application might return unexpected data or not function. Customizations that can make a mobile enterprise application inoperative include changes to an EnterpriseOne form in Form Design Aid (FDA) or fields modified with global data dictionary overrides—overrides with no specified jargon or language.

To resolve this issue, Oracle provides a comparison utility called the JDE JSON Mapping Tool. This tool enables you to compare and identify mismatched fields between the mobile enterprise application and EnterpriseOne, and remap the fields through AIS endPoint mappings.

2.4.1.1 How AIS endPoint Mappings Work

JD Edwards EnterpriseOne mobile enterprise applications are developed based on the JSON output returned from a specific EnterpriseOne environment. For mobile enterprise applications to function properly, the client (mobile enterprise application) must receive JSON responses from the AIS Server (server JSON) that match the expected responses in the client. This is referred to as the client contract.

To generate modified JSON output, the system uses an AISEndPoint.xml file deployed to the EnterpriseOne AIS Server. The AISEndPoint.xml file contains ID mappings in endPoint elements. The ID mappings map the fields expected in the mobile enterprise application client to the fields being sent by the AIS Server for each EnterpriseOne form.

> **Note:** The AISEndpoint.xml file is included in the AIS deployment object (war file).

In the AISEndPoint.xml file, the endPoint mapping is organized in a hierarchy that is equal to the hierarchy of an EnterpriseOne application form, which follows this order:

1. Form inputs for the main form or the parent form.
2. Any additional forms, which can be the main form or subforms.
3. Any form data controls, form action controls, or a grid within a form.
4. Any columns within a grid.

The AIS Server uses an endPoint mapping to transform the IDs used for both the input and output of a form service request. For input, the requested form IDs and all the IDs used in any grid or form action are replaced with values the server is expecting. For output, all of the IDs within the JSON response for the form are replaced with values expected by the mobile enterprise application client. Hence the "server" and "client" attributes in the mapping.

Transformations occur only when the application and form listed in the endPoint "module" parameter in the endPoint mapping match the application and form ID requested in the "formName" parameter of the service call. The module might not match the value in the "appOID" parameter. In this case, if the module matches the requested form name, the AIS Server will execute the form defined in the appOID, calling a different form than the form listed in the "formName" parameter.

The following example shows an endPoint mapping in the AISEndPoint.xml file.

Example 2–1 Example of an AIS Endpoint Mapping

```
<processingOptions appIdClient="P87NLPF1" appIdServer="P87NLPF1">
 <option longClient="dtSDFromDate1_34" longServer="dtSDFromDate_3"/>
   <option longClient="nInteger015_55" longServer="nInteger01_5"/>
  </processingOptions>

<endPoint module="P87TEST_W87NLPFA" appOID="P87NLPF_W87NLPFA" type="JAS">
```

```
  <mapping>
   <!--Form Inputs - both server and client required -->
     <formInput client="3" server="1"/>
     <formInput client="4" server="2"/>

<!--Forms - both server and client required, 0 is the id of the parent form for
power forms -->
      <form client="0" server="0">
<!--controlData - both short and long names required with ids -->
            <controlData longClient="txtEnterpriseOneEventPoint01_46"
                             longServer="txtEnterpriseOneEventPoint01_36"/>
            <!--controlAction - both client and server ids required -->
            <controlAction client="95" server="15"/>
<!--Grid columns - both server and client required, both short and long names
required -->
<column longClient="sPhoneType_89"
                            longServer="sPhoneType_25"/>
                </grid>
            </form>
<!--Forms - both server and client required, subforms have non-zero ids -->
            <form client="66" server="26">
                <controlAction client="30" server="50"/>
                < controlData longClient="txtEnterpriseOneEventPoint01_99"
                             longServer="txtEnterpriseOneEventPoint01_36"/>
                <grid client="20" server="20">
      <column    longClient="sPhoneType_88"
                            longServer="sPhoneType_25"/>
                </grid>
            </form>
        </mapping>
    </endPoint>
```

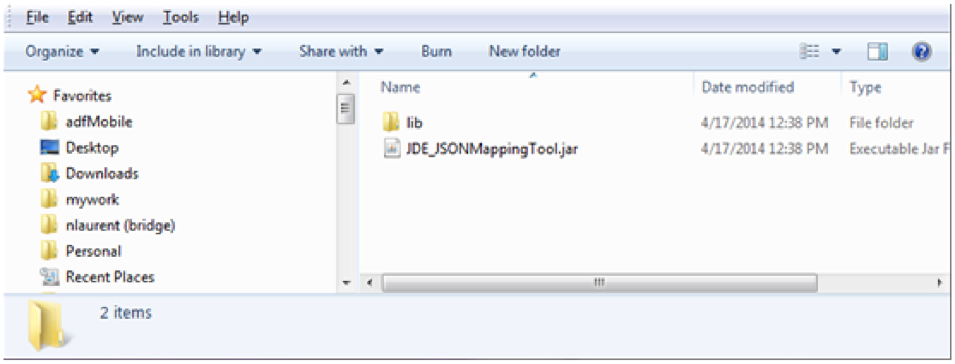
2.4.2 Using the JDE JSON Mapping Tool to Map Mismatched Fields

The JDE JSON Mapping Tool enables you to update the AISEndPoint.xml file with the proper JSON client-server mappings. After updating the AISEndPoint.xml file, you deploy it to the AIS Server to produce the expected JSON responses. The tool enables you to:

- Map mismatched fields to the current fields in the EnterpriseOne form.
- Save the mappings to a file so that later, you can incorporate the mappings into the AISEndPoint.xml file.

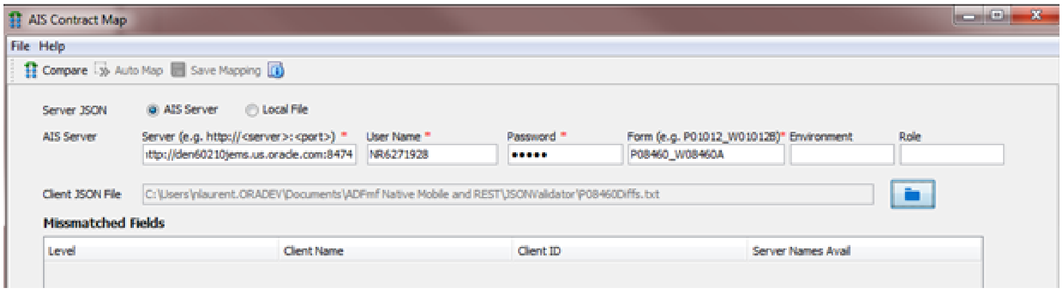
To map mismatched fields:

1. Locate the JDE_JSONMappingTool.zip file and unzip it to your local machine.



Name	Date modified	Type
lib	4/17/2014 12:38 PM	File folder
JDE_JSONMappingTool.jar	4/17/2014 12:38 PM	Executable Jar F

2. Double-click the jar file to launch the application.



Server JSON ● AIS Server ○ Local File

AIS Server

Server (e.g. http://<server>:<port>) *: ttp://den60210jems.us.oracle.com:8474

User Name *: NR6271928

Password *: •••••

Form (e.g. P01012_W01012B)*: P08460_W08460A

Environment:

Role:

Client JSON File: C:\Users\nlaurent.ORADEV\Documents\ADFmf Native Mobile and REST\JSONValidator\P08460Diffs.txt

Missmatched Fields

Level	Client Name	Client ID	Server Names Avail

3. Complete the following fields to identify the location of the server JSON information:

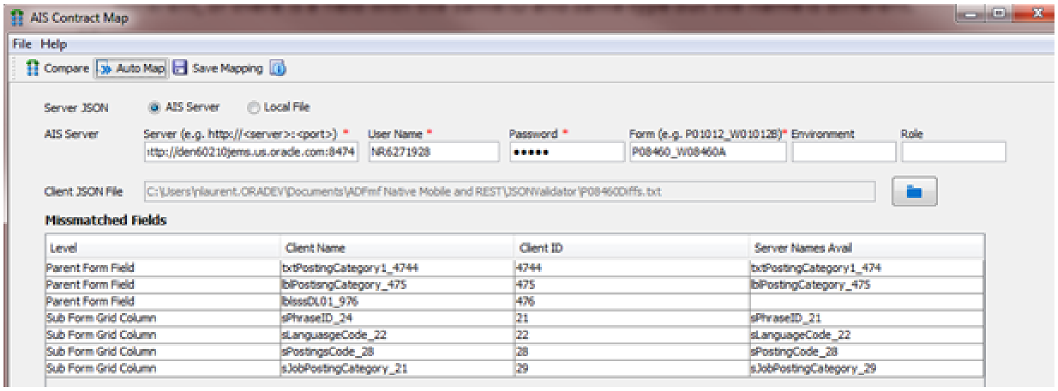
   - **Server**. Enter the path to the server where the AIS Server is deployed, for example: `http://<server>:<port>`
   - **User Name**. Enter a user name for the EnterpriseOne HTML Server.
   - **Password**. Enter a password for the EnterpriseOne HTML Server.
   - **Form**. Use the following syntax to identify the form for which you want to compare form service responses:

     `<application ID>_<form ID>`. For example: `P08460_W08460A`
   - **Environment**.
   - **Role**.

   > **Note:** You can also select the Local File option if you have the file with server JSON information on your local machine.

4. In the Client JSON File field, click the folder button to select the locally stored file with the client contract, which contains the client's expected JSON response for that form.

5. Click the **Compare** button in the menu bar. The tool displays any mismatched fields in the grid.



Server JSON ● AIS Server ○ Local File

AIS Server

Server (e.g. http://<server>:<port>) *: ttp://den60210jems.us.oracle.com:8474

User Name *: NR6271928

Password *: •••••

Form (e.g. P01012_W01012B)*: P08460_W08460A

Environment:

Role:

Client JSON File: C:\Users\nlaurent.ORADEV\Documents\ADFmf Native Mobile and REST\JSONValidator\P08460Diffs.txt

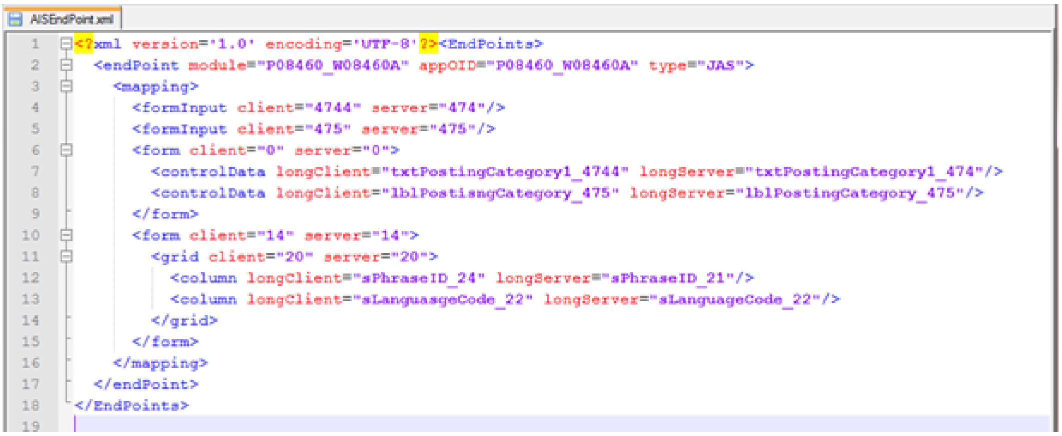
Missmatched Fields

Level	Client Name	Client ID	Server Names Avail
Parent Form Field	txtPostingCategory1_4744	4744	txtPostingCategory1_474
Parent Form Field	lblPostisngCategory_475	475	lblPostingCategory_475
Parent Form Field	lblssDL01_976	476	
Sub Form Grid Column	sPhraseID_24	21	sPhraseID_21
Sub Form Grid Column	sLanguasgeCode_22	22	sLanguageCode_22
Sub Form Grid Column	sPostingsCode_28	28	sPostingCode_28
Sub Form Grid Column	sJobPostingCategory_21	29	sJobPostingCategory_29

6. Click the **Auto Map** button to map the fields automatically.

   Auto Map matches fields where only the ID is different, or it matches fields that have the same ID and type but different names.

7. Review the mappings and map any remaining mismatched fields manually by using the drop-down menu in the Server Names Avail column.
8. Click the **Save Mapping** button and enter a unique name to save the xml file as a new file. Later, you must manually copy the endpoint information from this file into AISEndPoint.xml file.
9. Click **OK** on the confirmation message.
10. Open the xml file to review and verify the output.



```
<?xml version='1.0' encoding='UTF-8'?><EndPoints>
  <endPoint module="P08460_W08460A" appOID="P08460_W08460A" type="JAS">
    <mapping>
      <formInput client="4744" server="474"/>
      <formInput client="475" server="475"/>
      <form client="0" server="0">
        <controlData longClient="txtPostingCategory1_4744" longServer="txtPostingCategory1_474"/>
        <controlData longClient="lblPostisngCategory_475" longServer="lblPostingCategory_475"/>
      </form>
      <form client="14" server="14">
        <grid client="20" server="20">
          <column longClient="sPhraseID_24" longServer="sPhraseID_21"/>
          <column longClient="sLanguasgeCode_22" longServer="sLanguageCode_22"/>
        </grid>
      </form>
    </mapping>
  </endPoint>
</EndPoints>
```

11. Follow the instructions in the Modifying and Deploying AIS Field Mappings section to deploy the updated mappings.

2.4.3 Modifying and Deploying AIS Field Mappings

Perform the following tasks to modify and deploy AIS field mappings:

- Locate and Save the AIS Server Component JAR File as a New JAR
- Modify the AISEndpoint.xml in the AIS Server Component JAR File
- Use Server Manager to Deploy the New JAR File with the Updated AISEndpoint.xml to an AIS Server Instance

2.4.3.1 Locate and Save the AIS Server Component JAR File as a New JAR

To do so:

1. Locate the JAR file, which should be named similar to this: `E1_AISServer_9.1.4.6_03-13-2014_12_48.jar`.

   This is the same JAR file used to deploy the AIS Server.

2. Copy the JAR file to your local machine, renaming the file to differentiate it from the original.

2.4.3.2 Modify the AISEndpoint.xml in the AIS Server Component JAR File

Update the AISEndpoint.xml file in the new JAR file with the endPoint mappings from the mapping file generated from the JDE JSON Mapping Tool. To do so:

1. Use a zip utility to open the archive.

> **Note:** If you use 7-zip, you can open it (without unzipping it) and drill down to the folder that contains the JAR file, edit the JAR file, and then save it. If you use another zip utility, you may have to unzip the archive, edit the JAR file, and then rezip it.

2. In an editor, open the AISEndPoint.xml, which you can find in the following location:

   ```
   \E1_AISServer_Release_Name_
   ReleaseDate.jar\JDERestProxy.ear\JDERestProxy.war\WEB-INF\classes\
   ```

   With Release 9.1.5.5, the location of the AISEndPoint.xml has changed.

   If you do not have the file path to the XML files defined in the Server Manager configuration settings for AIS, you can directly deploy the AISEndPoint.xml file as always, but in this location in the war file:

   ```
   \E1_AISServer_Release_Name_
   ReleaseDate.jar\JDERestProxy.ear\JDERestProxy.war\WEB-INF\classes\Conf
   iguration\
   ```

   If you defined the path to the XML files in Server Manager, you do not need to modify the deployment. Simply place the AISEndPoint.xml file directly in the folder defined in the configuration.

   If you defined the path to the XML files in Server Manager, and you choose to not place the AISEndPoint.xml file in that location, the system will still look for the AISEndPoint.xml file in the deployment JAR file.

3. In an editor, open the mapping file generated by the JDE JSON Mapping Tool.

4. In the mapping file, copy each `<endPoint>` section from the start tag to the end tag, and paste it into the AISEndPoint.xml as a child of the `<EndPoints>` element.

5. After you modify it, save and close it. If a message box appears asking if you want to update the modified file, click **OK**.

2.4.3.3 Use Server Manager to Deploy the New JAR File with the Updated AISEndpoint.xml to an AIS Server Instance

To do so:

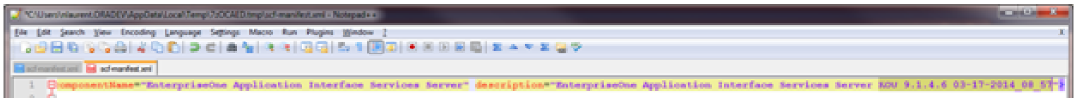
1. In the JAR file, update the date and time.

2. Navigate to the top level of the JAR file. Click **OK** if any dialog boxes appear asking if you want to update files in the archive.

3. Right-click the scf-manifest.xml file and select **Open**.

4. At the top of the file, modify the description attribute to uniquely identify it.

   The following screen shot shows an example of an scf-manifest.xml file with an updated description and time:


*C:\Users\rlaurent.ORADEV\AppData\Local\Temp\7zOCAED.tmp\scf-manifest.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
scf-manifest.xml
scf-manifest.xml

```
componentName="EnterpriseOne Application Interface Services Server" description="EnterpriseOne Application Interface Services Server XOU 9.1.4.6 03-17-2014_08_57-
```

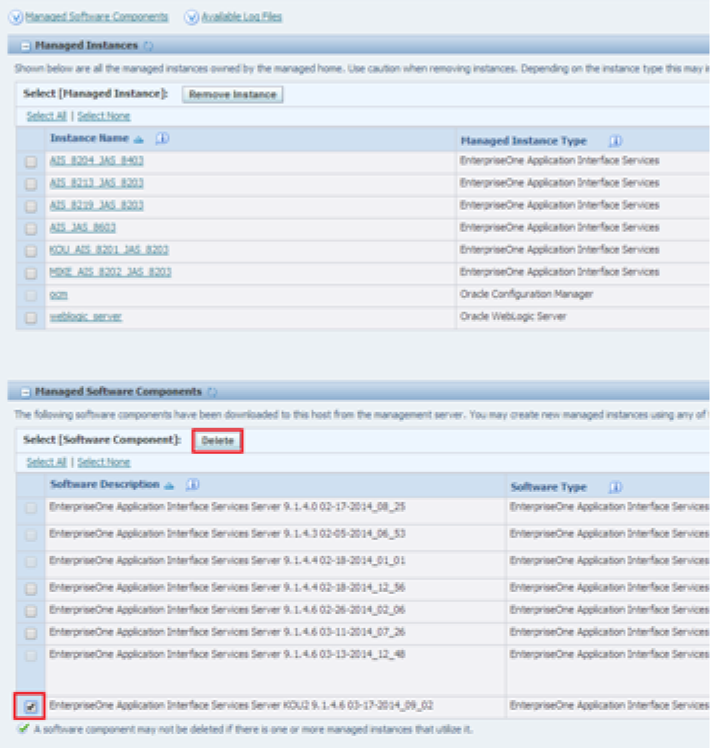
5. Save and close the file. Click **OK** if a dialog box appears asking if you want to update the archive.

6. Close the archive or rezip the files into the archive, depending on the zip utility you are using.

7. Access Server Manager.

8. Find the AIS Server managed instance and click the **Change** button to change the software version to the following base version if it is not already set:

   EnterpriseOne Application Interface Services Server 9.1.4.6 03-13-2014_12_48



Managed Instances

Shown below are all the managed instances owned by the managed home. Use caution when removing instances. Depending on the instance type this may i

Select [Managed Instance]: Remove Instance

Select All | Select None

	Instance Name	Managed Instance Type
□	AIS_8204_JAS_8403	EnterpriseOne Application Interface Services
□	AIS_8213_JAS_8203	EnterpriseOne Application Interface Services
□	AIS_8219_JAS_8203	EnterpriseOne Application Interface Services
□	AIS_JAS_8603	EnterpriseOne Application Interface Services
□	KOU_AIS_8201_JAS_8203	EnterpriseOne Application Interface Services
□	MIKE_AIS_8202_JAS_8203	EnterpriseOne Application Interface Services
□	ocm	Oracle Configuration Manager
□	weblogic_server	Oracle WebLogic Server

Managed Software Components

The following software components have been downloaded to this host from the management server. You may create new managed instances using any of

Select [Software Component]: Delete

Select All | Select None

	Software Description	Software Type
□	EnterpriseOne Application Interface Services Server 9.1.4.0 02-17-2014_08_25	EnterpriseOne Application Interface Services
□	EnterpriseOne Application Interface Services Server 9.1.4.3 02-05-2014_06_53	EnterpriseOne Application Interface Services
□	EnterpriseOne Application Interface Services Server 9.1.4.4 02-18-2014_01_01	EnterpriseOne Application Interface Services
□	EnterpriseOne Application Interface Services Server 9.1.4.4 02-18-2014_12_56	EnterpriseOne Application Interface Services
□	EnterpriseOne Application Interface Services Server 9.1.4.6 02-26-2014_02_06	EnterpriseOne Application Interface Services
□	EnterpriseOne Application Interface Services Server 9.1.4.6 03-11-2014_07_26	EnterpriseOne Application Interface Services
□	EnterpriseOne Application Interface Services Server 9.1.4.6 03-13-2014_12_48	EnterpriseOne Application Interface Services
☑	EnterpriseOne Application Interface Services Server KOU2 9.1.4.6 03-17-2014_09_02	EnterpriseOne Application Interface Services

✓ A software component may not be deleted if there is one or more managed instances that utilize it.

9. Go to the managed home and delete the previous component that was assigned to your server.

10. In the left pane, select **Manage Software**, and then click the **Choose File** button.

11. Select the file you just modified, and then click the **Upload** button.

12. If you receive the following message, delete any existing uploads that were based on the same JAR. This will not affect any current deployments.

    ```
    "Caution: The uploaded file already exists in the management console.
    The uploaded file has been discarded."
    ```

    After uploading the file, you need to distribute it.

13. To distribute the file, select the managed home with the AIS Server instances. If the check box for the AIS Server instance is not selected, then you need to perform steps b and c.

14. Go to your managed instance and stop it.

15. For the Software Component Version, click the **Change** button, select the new one you just distributed, and then click the **Change Component** button.

    Server Manager automatically restarts the server.

16. Test the updated mappings by running the mobile enterprise application. If the application functions properly, you have successfully updated the mappings.

3

Additional Tasks to Implement EnterpriseOne Mobile Enterprise Applications

EnterpriseOne mobile enterprise applications are extensions of the base applications in the EnterpriseOne system. In EnterpriseOne, you must set up mobile enterprise application versions, as well as processing options and security for both the mobile enterprise applications and the base EnterpriseOne applications used by the mobile applications. These settings determine the EnterpriseOne users authorized to access mobile enterprise applications, as well as the data users can work with in their mobile enterprise applications.

This chapter contains the following topics:

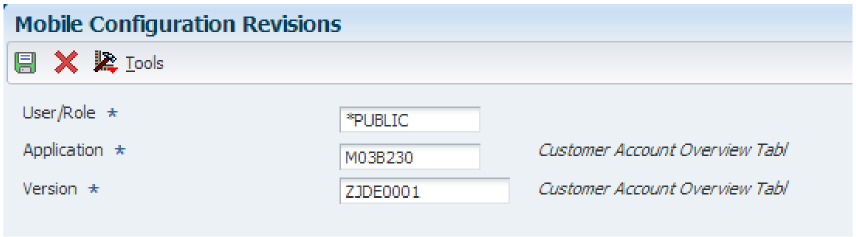
- Section 3.1, "Defining Mobile Enterprise Application Versions for Mobile Users"
- Section 3.2, "Specifying Processing and Display Options for Mobile Enterprise Applications"
- Section 3.3, "Setting Up Security for EnterpriseOne Mobile Enterprise Applications"
- Section 3.4, "Setting Up Security for Base EnterpriseOne Applications Used by Mobile Enterprise Applications"

3.1 Defining Mobile Enterprise Application Versions for Mobile Users

In EnterpriseOne, use the Mobile Version Management program (P98950M) to set up version information for mobile enterprise applications. You define which versions of the mobile enterprise application each user in your organization will use when they log into a mobile enterprise application. You can set up one default version for all users, or you can set up multiple versions for different roles or for specific users.

To access P98950M, click the Navigator menu, EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, Mobile Management, and then Mobile Version Management.

1. On Mobile Version Management - Work With Mobile Configuration, click **Add**.



User/Role *	*PUBLIC	
Application *	M03B230	Customer Account Overview Tabl
Version *	ZJDE0001	Customer Account Overview Tabl

2. On Mobile Configuration Revisions, complete the following required fields and then click **OK**:

   - **User/Role:** Enter the user ID or the role that you want to assign to a specific version of a mobile application. If you want all users of the application to use the same version, enter *PUBLIC in this field.
   - **Application:** Enter the mobile program for which you are setting up a version. For example, enter M03B230 to set up a version for the Customer Account Overview Tablet application.
   - **Version:** Enter the version that you want the specified user or role to use when accessing the mobile application.

   Note: You cannot edit mobile configuration records. If you need to update a record, delete the record and enter a new record with the updated information.

3.2 Specifying Processing and Display Options for Mobile Enterprise Applications

Set up processing options to specify which versions of the base EnterpriseOne applications the mobile enterprise applications use. Also, some mobile applications use processing options or display preferences to determine what is displayed in the application.

See the *JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implementation Guide* for instructions on how to set up processing and display options.

3.3 Setting Up Security for EnterpriseOne Mobile Enterprise Applications

Set up security for mobile enterprise applications using the standard application security in the EnterpriseOne Security Workbench. Application security can be defined by user, role, or using *PUBLIC (all users). You set up application security for the *version* of the mobile enterprise application that you defined, as described in the Defining Mobile Enterprise Application Versions for Mobile Users section in this guide.

In the Security Workbench, the only application security option that applies to mobile enterprise applications is the "Run" security option.

For instructions on how to set up application security in EnterpriseOne, see "Managing Application Security" in the *JD Edwards EnterpriseOne Tools Security Administration Guide*.

For a list of mobile enterprise applications that you need to secure, see the *JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implementation Guide*.

3.4 Setting Up Security for Base EnterpriseOne Applications Used by Mobile Enterprise Applications

In addition to setting up permissions to access EnterpriseOne mobile enterprise applications, you must make sure that mobile users have permissions to access the base EnterpriseOne applications and application data that the mobile enterprise applications use.

In the Enterpriseone Security Workbench, the following types of security applied to base EnterpriseOne applications persist to mobile enterprise applications:

- Application security
- Exclusive application security
- Row security

  If row security is defined that prevents users from seeing certain data in the base EnterpriseOne application, mobile users will not be able to see the data in the mobile enterprise application.

For more information about how to review and set up security records for the types of security in the preceding list, see "Setting Up Authorization Security with Security Workbench" in the *JD Edwards EnterpriseOne Tools Security Administration Guide*.

For a list of base EnterpriseOne applications used by each mobile enterprise application, see the *JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implementation Guide*.

4

Troubleshooting Mobile Enterprise Applications

This chapter contains the following topics:

- Section 4.1, "Login Issues"
- Section 4.2, "Mobile Enterprise Application Issues"

4.1 Login Issues

Login Fails After User Launches the Mobile Enterprise Application

If the login fails after a mobile user launches the mobile enterprise application and enters the URL to connect to the server:

- Make sure the mobile user has the correct URL. See Deploying and Managing the AIS Server through Server Manager in this guide for more information.
- Make sure the AIS Server is up and running on the port specified in the deployment settings in Server Manager.
- If the AIS Server is running, perform the following test to confirm that it is responding to requests:

  1. In Server Manager, access the AIS Server instance.
  2. Click the **Test Connection** link.

     The resulting page shows the environment, role, and HTML Server.
  3. Verify the settings in the resulting page against the settings for the AIS Server in Server Manager. If the settings are not in synch, correct any of the settings in Server Manager, test the connection, and then restart the AIS Server instance.

- Make sure the HTML Server setting for the Allowed Hosts is configured properly. See Configuring the Allowed Hosts Setting for the EnterpriseOne HTML Server in this guide for more information.
- Depending on the configuration of the AIS server that supports your organization's mobile applications, you might be required to sign into VPN on your mobile device before you can sign into a mobile application. Contact your system administrator to determine if this step is required.

Application Not Compatible with Server Error Message

After logging in, the following message appears:

"This application is not compatible with the server you are connected to."

The user will not be able to continue using the application. The administrator must upgrade the EnterpriseOne Tools release to a compatible level for the application.

For a list of the EnterpriseOne mobile enterprise applications and the minimum EnterpriseOne Tools release required to run them, see the following document on My Oracle Support (login required):

Information Center for JD Edwards EnterpriseOne Mobile Applications (Doc ID 1637232.2)

`https://support.oracle.com/epmos/faces/DocumentDisplay?id=1637232.2`

4.2 Mobile Enterprise Application Issues

Data Dictionary Item with Global Override Causes Mobile Enterprise Application to Not Work as Desired

If a mobile enterprise application references a data dictionary (DD) item in EnterpriseOne, and the customer has updated the DD item in EnterpriseOne with a global override of the DD item description, the mobile enterprise application will throw a null pointer exception or an undefined error. The result is that the mobile enterprise application will not receive values from EnterpriseOne and the application will not work as desired.

A global override of the DD item description overrides a data item's row description and is not specific to any language or Jargon Code (system code). To fix this issue, in EnterpriseOne, remove the global override of the description and specify description overrides only for a specific language or Jargon Code. See "Understanding Jargon and Alternate Language Terms" in the *JD Edwards EnterpriseOne Tools Data Dictionary Guide* for more information.

Unable to View Data or Application Features

If login is successful, but users cannot see data or application features:

- Make sure mobile users have the proper security permissions to access the EnterpriseOne mobile enterprise application.
- Make sure mobile users have the proper security permissions to access the EnterpriseOne application used by the mobile enterprise application.
- Make sure mobile users have the proper security permissions to access the data in the EnterpriseOne base application. If row security is defined that prevents users from seeing certain data in the base EnterpriseOne application, mobile users will not be able to see the data in the mobile enterprise application.

See the following topics in this guide for more information:

- Setting Up Security for EnterpriseOne Mobile Enterprise Applications
- Setting Up Security for Base EnterpriseOne Applications Used by Mobile Enterprise Applications

Unable to Work with Attachments

If you cannot work with media object attachments in a mobile enterprise application that supports attachments, you need to make sure that media object attachments are properly configured in the base EnterpriseOne application. Refer to the applicable base EnterpriseOne application documentation for more information. Use the following link to access the JD Edwards EnterpriseOne Applications Documentation Library:

http://docs.oracle.com/cd/E16582_01/index.htm